

REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 2-21 were pending in this application. Claims 2, 15, and 20 have been amended. Accordingly, claims 2-21 will be pending herein upon entry of this Amendment. Support for the amendment claims 2, 15, and 20 can be found, for example, in paragraphs 16 and 39 of the application. For the reasons stated below, Applicants respectfully submit that all claims pending in this application are in condition for allowance.

Examiner Tran is thanked for the courtesies extended to Applicants' representative during the telephone call on April 20, 2005.

In the Advisory Action, the Examiner has again analogized the "substitute process creation function" of claims 2, 15, and 20 to the network security detector of Shostack et al. U.S. Patent No. 6,298,445 (hereinafter "Shostack"). The Examiner has also analogized the "user-mode-application" of claims 2, 15, and 20 to the network security detector of Shostack and the email service of Shostack. Applicants submit that these analogies are incorrect and inconsistent.

The "substitute process creation function" in the present invention is inserted into the kernel of the operating system once and is used to allow or block execution of all executables scheduled for execution by the operating system of a computer (paragraph 38). These executables are already stored on the computer running the operating system. Potentially malicious executables are blocked by the substitute process creation function just before being executed by the operating system in response to a user request to execute the executables. In

other words, all actions to prevent the execution of malicious software occur within the operating system.

In contrast, the network security detector of Shostack scans the network for violators (column 6, 44-46). The network security detector does not work at the operating system level. The network security detector works at the network level and checks packets rather than contiguous executables.

The Examiner has also analogized the “user-mode application” of claims 2, 15, and 20 to the network security detector of Shostack. The Examiner suggests that “‘intercepting a request’ is inherent in the installation process that first installs the software enhancement onto a separate storage device then performs checks to insure authentic software and user verification before unlocking any software enhancement.”

In the present invention, the “user-mode application” is a service running on the same operating system and computer as the “substitute process creation function” (paragraph 16). The purpose of the “user-mode application” is to communicate with the “substitute process creation function” within the operating system and provide an allow or block ruling to the “substitute process creation function” (paragraph 39).

It does not make sense, as the Examiner has suggested, that the network security detector is both the user-mode application and the substitute creation function. If this were the case, there would be no need for communication between the user-mode application and the substitute creation function.

The Examiner has also suggested that the “user-mode application” is analogous to an email service. Again, an email service implies that there is communication across a network, which is not the type of communication between the user-mode application and the substitute creation function described and claimed in the present application.

Applicants respectfully submit that it is inconsistent to equate the “user-mode application” to the network security detector, on the one hand, and to an email program communicating with the network security detector, on the other hand. Moreover, it is emphasized that the claims of the present application are directed to a method of detecting malicious software within an operating system and not over a network.

With the foregoing in mind, and in an effort to even further clarify the features of the present invention, independent claims 2, 15, and 20 have been amended to specify that the user-mode application is running as a service on the operating system and the communication between the user-mode application and the substitute process creation function takes place within the operating system. None of the references cited by the Examiner either alone or in combination teaches that the user-mode application is running as a service on the operating system and the communication between the user-mode application and the substitute process creation function takes place within the operating system. Accordingly, Applicants respectfully submit that amended claims 2, 15, and 20 are allowable over the prior art of record. Dependent claims 3-14,16-19, and 21 are also allowable for at least the same reasons.

In view of the foregoing all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is

Serial No.: 09/821,754
Art Unit: 2134

Attorney's Docket No.: CIG-101
Page 11

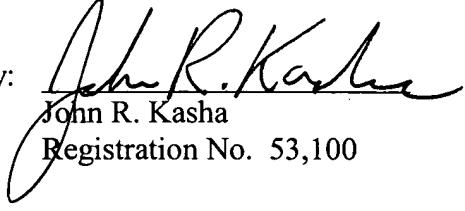
desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone applicants' undersigned representative at the number listed below.

PILLSBURY WINTHROP
SHAW PTTMAN LLP
1650 Tysons Boulevard
McLean, VA 22102
Tel: 703/770-7900

Respectfully submitted,
SCHMID ET AL.

Date: June 7, 2005

By:


John R. Kasha
Registration No. 53,100

Attachments:

JRK/src

Customer No. 28970